Scanning for Vulnerabilities: Is it lawful?

Andrew Cormack
What “law”?
Article 2:

“Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right”

Directive 2013/40/EC has same “access without right” wording
Optional Extras

• Security measures
  – “Party may require that the offence be committed by infringing security measures”
  – EU Directive 2013/40 also includes this
  – i.e. No security measure => no offence

• Intention
  – “...with the intent of obtaining computer data or other dishonest intent”
  – i.e. Honest intention => no offence

• UK doesn’t have either of these, you may
“Access without Right”
What is “Access”? 

- It depends
  - Some theories/cases say any “approach” (e.g. war dialling)
  - Others only if you get “inside”
    - Thinking of a computer like a house/trespass
- UK law says “causes a computer to perform any function”
  - Scanning needs a response: i.e. that target performs a function!
What grants “Right”/“Authorisation”?

• Explicit permission, obviously
• But must be more
  – Otherwise following Google links would be a crime!
• Maybe advertising (e.g. www.)? Or connecting to network?
• UK cases imply connecting is sufficient, but
  – Spaming is not a crime (Yarimaka)
  – Directory traversal is (R v Cuthbert)
  – So, maybe only things related to intended function?
    • A test originating in the US v Morris worm trial!
Applying that...
UK tentative conclusion (YMWV)

• According to legislation (*Computer Misuse Act 1990*)
  – Scanning is access
  – Even if ‘victim’ has no security measures
  – Intention is not relevant, whether honest or dishonest

• Case law suggests
  – IP connection => implied “authorisation”
    • For (parts of) normal function
    • Until you get a positive “denied” response
  – Neither case creates legal precedent 😞

• But cases seem to imply
  – TCP connection is authorised
  – UDP command is authorised (NTP amplifier)
  – Buffer overflow isn’t (Heartbleed)
Same questions:
• Is scanning access?
• Is there a “technical barrier” test?
• Is there an “intention” test?
• What authorisation/right can be presumed?